УТВЕРЖДАЮ
Начальник управления ветеринарии Ростовской области

С.Н. Карташов

« 23 » мая 2013 г.

ИНСТРУКЦИЯ

по парольной защите информационных систем персональных данных управления ветеринарии Ростовской области

1. Общие положения

Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных систем персональных данных (далее - ИСПДн) управления ветеринарии Ростовской области (далее - управление), защищенной от несанкционированного доступа, а также порядок контроля за действиями пользователей при работе с паролями.

2. Парольная политика

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей при работе с паролями возлагается на администратора информационной безопасности (далее - ИБ).

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДн самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее шести символов;

– в числе символов пароля обязательно должны присутствовать только цифры и/или буквы в верхнем или нижнем регистрах;

– символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее

чем в шести позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

При наличии необходимости и с целью обеспечения технологической возможности использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения вместе с именами соответствующих учетных записей в запечатанном конверте или опечатанном пенале передавать на хранение администратору безопасности информации или своему руководителю. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать ответственного за защиту персональных данных на объекте.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности информации немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания руководителя предприятия.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности информации.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе администратора безопасности информации или начальника отдела.

Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации.

Доступ к настройкам BIOS рабочих станций ограничивается администратором ИБ с помощью пароля длиной не менее 6 символов. Данный пароль администратор ИБ не должен никому сообщать. Работу представителей организаций, осуществляющих аутсорсинг, разрешать только после собственноручного ввода пароля администратором. На время своего отсутствия администратор оставляет значения пароля входа в

ИСПДн и в настройки BIOS серверов и рабочих станций в закрытом и опечатанном конверте в сейфе.
